Approved by Governors: 06/2019
Next review: 06/2021

E-Safety Policy

1.0 Purpose

Marling School recognises its responsibility in providing good e-safety information and training to all its users. This Policy details the actions taken to promote e-safety at Marling School. This encompasses the use of new technologies, internet and electronic communications such as mobile phones and collaboration tools such as wikis and social networking.

2.0 Scope

E-Safety in school depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students
- Sound policy implementation to include education, published policies, network design and usage
- Safe and secure broadband with effective filters
- Making clear the rules for Internet usage and all electronic communications

This policy is intended to create awareness of the need to educate students about the benefits and risks of using technologies; and to explain how we protect children from unsuitable material.

It is the duty of the school to ensure that every child in their care is safe, and the same principles apply to the 'virtual' or digital world as would be applied to the school's physical site.

3.0 Responsibilities

The Governing Body is responsible for ensuring that:

- The School's E-Safety Policy is maintained and updated regularly
- That procedures and strategies related to the policy are implemented

The Headteacher and Senior Leadership Team (SLT) are responsible for:

- Maintaining this policy, providing advice and guidance on its implementation
- Ensuring that staff are aware of their responsibilities and are given relevant training and support

E-Safety Coordinator is responsible for:

- Advice to SLT on all aspects of e-safety
- Supporting HoDs, HoYs and SLT in investigating breaches of the E-Safety Policy
- Lead on the design and delivery of e-safety education to students
- Lead on the design and delivery of e-safety education to parents
- Lead on the design and delivery of e-safety training to staff and governors

The IT Services Manager and IT staff are responsible for:

- Security of the school information systems which will be reviewed regularly via the IT Services Manager
- Monitoring the school's system and reporting breaches of the E-Safety policy to the SLT
- Advising and supporting the staff in dealing with e-safety issues in the school

All staff have a responsibility for:

- Ensuring that they maintain their awareness and knowledge of e-safety concerns
- Demonstrating best practice
- Dealing with incidents of breaches in the E-Safety Policy
- Reporting incidents of breaches in the E-Safety policy within the school
- Educating students about the risks of not being e-safe
- Engaging in training events on e-safety

Students are responsible for:

- Behaving in a way that does not put themselves or others at e-safety risk
- Follow all e-safety rules including the Responsible Use Policy and instructions of staff
- Promoting e-safety amongst their peers by adopting best practice

Visitors must:

- Sign in on arrival and out on departure at the School Office
- Read the resume of the Safeguarding procedures on arrival at the School
- Accept the Responsible Use Policy
- Follow the instructions of staff when on site or accessing the school's IT system

4.0 Principles

The Internet is an essential tool in life for education, business and social interaction. The school will aim to provide students with effective Internet access as part of their learning process.

All school Internet access is designed for student use and will include filtering appropriate to the age of the students and subjects being studied.

All staff should be familiar with the school's guiding principles including:

- Safe use of e-mail
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network
- Safe use of school network, equipment and data
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras
- Publication of student information/photographs and use of website
- E-Bullying / Cyberbullying procedures
- Their role in providing e-safety education for students

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-safety procedures. There should be a 'No Blame' culture so students feel able to report any bullying, abuse or inappropriate materials, in accordance with the Anti-bullying Policy.

This policy incorporates the school procedures and notes for guidance for e-safety outlined in the attached appendix. These procedures and guidance may be amended with the approval of the Senior Leadership Team. The Governors should be made aware of any changes via a report to the Student Progress Committee in the first instance.

The school will offer Parent Support and training that will help raise awareness of the risks and the ways to help their children understand the dangers.

The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of Internet access. Students are responsible for their internet use.

5.0 Links to other policies

Behaviour Policy
Anti-bullying Policy
General Complaints Policy
Prevention of Extremism and Radicalisation Policy
Responsible Use Policy – Main
Responsible Use Policy – Student
Safeguarding Policy

E-Safety Policy - Appendix 1

School procedures

SYSTEMS

- The security of the school information systems will be reviewed regularly via the IT Services Manager
- Unapproved system utilities and executable files will not be allowed in students' work areas or attached to e-mail
- User areas, Emails and files held on the school's network will be regularly checked. All files on the school system can be and will be accessed by the IT Services Manager when needed
- A message informing uses of the Responsible Use Policy will be displayed every time someone logs in
- Newsgroups and RSS feeds will be blocked unless a specific use is approved
- Malware protection on the schools systems will be updated continually and automatically by the security software. This will be managed by the IT Services Manager
- Portable media should not contain malicious, illegal or unlicensed executable files and should be virus checked

STAFF TRAINING

- All staff and students will be made aware that they should not use a machine with a cross on the Sophos shield and that they should report this to IT immediately
- Staff will be reminded/updated about e-safety matters at the start of each year

COMMUNICATION

- On a 'public-facing page' the publishing of students' names with their images is not acceptable without explicit written parental permission
- The school will block/filter access to social networking sites
- The forwarding of chain letters is not permitted on school systems
- Twitter may be used for school purposes, but only with a dedicated school account, linked to a school email address. If a school twitter account is used then it should follow no school member's private accounts. Anyone may follow it
- No use of school email should be made to subscribe to Social Networking (e.g. Facebook etc.…) except when authorised by the HT
- Any school social media accounts, with a primary target audience of students, should begin with "Marling"
- All email contact between students and staff should be via their school e-mail account of the member of staff (The school is working toward a position in which student email accounts can be accessed remotely. Until this is possible students may email staff at their school email address using their private email address)
- E-mails sent to external organisations reflect upon the school and should therefore be appropriate at all times
- Images that include students should be selected carefully and should not enable individual students to be clearly identified
- Whenever a difficult or potentially ambiguous issue needs to be broached, it should be done in person and not by email
- The circulation list for any email should be kept as small as possible
- Emails should err towards brevity rather than being discursive
- Staff emails to large number of internal recipients should be routed via the line management structure
- There is a 20MB limit on email attachments
- Where possible attachments should not be forwarded via emails to large number of colleagues. Staff should instead be directed to the relevant document via a hyperlink
- Staff and Students should not be 'friends' on Social Networking Sites or Instant Messaging services
- Care should be taken if friending parents or recently-ex-students
- Bluetooth should be switched off when not in use, and in school or on school activities unless authorized by the supervising member of staff

- Staff contact with Parents and students via phone should be made from a school phone and not a personal phone. Where this is not possible the phone caller ID should be disabled
- Pictures should be taken from school cameras and not personal cameras or phones, except in rare circumstances. Where a personal camera is used, the photographs should be transferred directly to the school system and the camera storage erased
- If a student is directed to post on public sites by a member of staff, they should not post images and names together without prior parental consent. In addition, no private information (addresses, telephone numbers etc.) should be posted

INFRINGEMENTS

- Student breaches of the Responsible Use Policy or E-Safety policy will be dealt with as per the behaviour policy. The Head of Computing will act as the E-Safety Coordinator and advise Departmental Heads, Pastoral Leaders and SLT
- Any complaint about staff misuse will be reported to the HT. The Head of Computing will support the Assistant Headteacher who acts as E-Safety Coordinator and advise Departmental Heads, Pastoral Leaders and SLT
- Staff and students are given information about infringements in use and possible sanctions which may include referral to the Police. More details can be found in the Responsible Use Policy. The school always cooperates with the investigating authorities
- Complaints of cyber bullying are dealt with in accordance with our Anti-Bullying Policy.
  - Complaints related to child protection are dealt with in accordance within the school's Safeguarding policy.
- Students must immediately report it if they receive offensive e-mail to a member of staff

Commented [m1]: Is this still the case?

E-Safety Policy - Appendix 2

Notes for Guidance

STUDENT EDUCATION ABOUT E-SAFETY

- Students are taught about acceptable Internet usage in discrete Computing lessons and though all ICT based lessons and are expected to meet the objective outlined in the policy
- Students are taught how to research effectively using the Internet
- Students are taught about copyright and creative commons obligations and are expected to comply with the legislation
- ICT based lessons will play an active part in e-safety education
- Students are taught how to evaluate the information they find, judging its validity and suitability for purpose
- Students should not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- Students will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc
- Students will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas
- Students will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others
- Students will be advised not to publish specific and detailed private thoughts
- An E safety group of key IT staff and representative from the student body will lead on the education of students and other stakeholders with regard to E-Safety. The brief of the group is to advise the SLT on current E-Safety issues, the most effective means with which to communicate E-Safety matters to students and staff and the content of the E-Safety Policy
- A series of assemblies will be delivered to all students each year to cover areas such as:
  - A basic intro to IT and the basic security precaution
  - A guide to what's in the Responsible Use Policy and what it means to them
  - Students rights and concerns around mobile phones
  - How to report E-Safety issues
  - How to use social networking safely
  - What is legal and illegal about IT use in school

PARENTAL ADVICE

- Excessive social e-mail use (for staff and students) can interfere with learning and may be restricted in school. Parents are advised to monitor student use at home
- An internet safety presentation should be offered to parents
- A presentation should be delivered to Year 6 parents about the ICT that Marling offers

Definitions:

Newsgroups	An online discussion forum
Bluetooth	Wireless communication protocol often available on portable devices
IM	Instant Messaging
Malware	Overarching term used to define Viruses, Trojan Horses, Spyware and other malicious software applications
RSS	Really Simple Syndication – a method of content distribution used by websites
Public Facing Web Site	Any site which is openly accessible via the internet in an anonymous way
ICT	Any lesson (across the curriculum) which uses computational or communications equipment